

AO 91 (Rev. 11/11) Criminal Complaint

SealedPublic and unofficial staff access
to this instrument are
prohibited by court order.

UNITED STATES DISTRICT COURT

for the

Southern District of Texas

United States District Court
Southern District of Texas
FILED

AUG 27 2019

David J. Bradley, Clerk of Court

United States of America)

v.)

Charles McCreary, Jr. aka "User 1") Case No.

and)

Scott Fucito aka "User 6")

H19-1602M

Defendant(s)

CRIMINAL COMPLAINT

I, the complainant in this case, state that the following is true to the best of my knowledge and belief.

On or about the date(s) of July 2018 - Present in the county of Harris in the
Southern District of Texas, the defendant(s) violated:

Code Section

Offense Description

18 U.S.C. 2252A(a)(2) and (b)(1)

Conspiracy to Recieve and Distribute Child Pornography

This criminal complaint is based on these facts:

See attached affidavit.

☒ Continued on the attached sheet.

Complainant's signature

Joshua Conrad, Special Agent HSI

Printed name and title

Sworn to before me and signed in my presence.

Date:

8/27/19



Judge's signature

City and state:

Houston, Texas

United State's Magistrate Judge Peter Bray

Printed name and title

AFFIDAVIT IN SUPPORT OF CRIMINAL COMPLAINT

I, Joshua Conrad, a Special Agent with Homeland Security Investigations, being duly sworn, depose and state as follows:

INTRODUCTION

1. I am a Special Agent (“SA”) with the Department of Homeland Security, Immigration and Customs Enforcement, Homeland Security Investigations (“HSI”), assigned to the Special Agent in Charge in Philadelphia, PA, and I have been so employed since April 2016. Prior to that, I was assigned to the Special Agent in Charge in El Paso, Texas, since October 2010. As part of my daily duties as an HSI agent, I investigate criminal violations relating to child exploitation and child pornography including violations pertaining to the illegal distribution, receipt, and possession of child pornography, in violation of 18 U.S.C. §§ 2251, 2252(a), and 2252A. I have had the opportunity to observe and review numerous examples of child pornography (as defined in 18 U.S.C. § 2256) in all forms of media including computer media. I have also participated in the execution of numerous search warrants, a number of which involved child exploitation and/or child pornography offenses.

2. This affidavit is made in support of a criminal complaint charging Charles McCREARY, JR., aka “User 1,” and Scot FUCITO, aka “User 6,” with conspiracy to distribute and receive in violation of 18 U.S.C. § 2252A(a)(2) and (b)(1).

3. I am familiar with the information contained in this Affidavit based upon the investigation I have conducted, and based on my conversations with other law enforcement officers who have engaged in numerous investigations involving child exploitation, and with other witnesses.

4. Because this Affidavit is being submitted for the limited purpose of demonstrating probable cause in support of the attached criminal complaint, I have not included each and every fact known to me concerning this investigation. I have set forth only those facts that I believe are necessary to establish probable cause.

STATUTORY AUTHORITY

5. Title 18 U.S.C. § 2252A(a) and (b)(1) prohibits a person from knowingly transporting, shipping, receiving, distributing, reproducing for distribution, possessing, or accessing with intent to view any child pornography, as defined in Title 18 U.S.C. § 2256(8), when such child pornography was either mailed or shipped or transported in interstate or foreign commerce, or in or affecting interstate commerce, by any means, including by computer, or when such child pornography was produced using materials that had traveled in interstate or foreign commerce, and any attempts or conspiracies to do so.

PROBABLE CAUSE

Investigation of Network 1, Network 2, and Network 3

6. On May 31, 2017, HSI SA Joshua Conrad created the undercover online identity “UC1”¹ to access Protocol A2 chat rooms on the Network 13 network. Protocol A chats are applications that facilitate communication by text. Protocol A chat rooms are mainly designed for group communication in discussion forums, but can also be used for private, one-on-one communications, data sharing, and file sharing.

¹ The real user name of UC1 is known to law enforcement but is being disguised in order to protect the ongoing investigation.

² The real name of Protocol A is known to law enforcement but is being disguised in order to protect the ongoing investigation.

³ The real name of Network 1 is known to law enforcement but is being disguised in order to protect the ongoing investigation.

7. SA Conrad, while in the Eastern District of Pennsylvania, used this undercover online identity to join and access multiple Protocol A Network 1 chat rooms, all of which were forums for potential targets interested in engaging in sexual activities with minors and trafficking in sexually explicit depictions of minors.

8. While SA Conrad was logged into Chat Room 1 on the Network 1 server, SA Conrad observed a user, "User 1",⁴ posting links to what appeared to be images of children engaged in sexually explicit conduct. These links were to third-party file-sharing websites. SA Conrad accessed several of these links and confirmed that the links led to child pornography images. User 1 was also changing chat room modes for other users, which indicated he had chat room administrative rights for Chat Room 1⁵. Within Protocol A, there are numerous chat room modes that function essentially as rules for how a chat room operates. For example, there is a chat room mode that can ban users with a particular nickname from joining a chat room and there is a chat room mode which makes the chat room invite-only. Other users in the chat room could see User 1's nickname or username. This username refers to the Protocol A username that User 1 designated as the name to display when the user was connected to Protocol A.

9. While SA Conrad was logged into Chat Room 1 on the Network 1 server, SA Conrad also observed a user, "User 2",⁶ posting links to what appeared to be images of children engaged in sexually explicit conduct. These links were to third-party file-sharing websites. SA Conrad accessed several of these links and confirmed that the links led to child pornography

⁴ The real user name of User 1 references a sexual interest in children and is known to law enforcement but is being disguised in order to protect the ongoing investigation.

⁵ The real name of Chat Room 1 is known to law enforcement but is being disguised in order to protect the ongoing investigation.

⁶ The real user name of User 2 is known to law enforcement but is being disguised in order to protect the ongoing investigation.

images. User 2 was also changing chat room modes for other users, which indicated he had chat room administrative rights for Chat Room 1. Other users in the chat room could see User 2's nickname or username. This username refers to the Protocol A username that User 2 designated as the name to display when the user was connected to Protocol A.

10. While SA Conrad was logged into Chat Room 1 on the Network 1 server, SA Conrad also observed a user, "User 3",⁷ changing chat room modes for other users, which indicated he had chat room administrative rights for Chat Room 1. User 3 also posted links to third-party file-sharing websites. SA Conrad accessed several of these links and confirmed that the links led to images involving child erotica. Other users in the chat room could see User 3's nickname or username. This username refers to the Protocol A username that User 3 designated as the name to display when that user was connected to Protocol A.

11. Protocol A has two tiers of administrators, a higher tier and a lower tier. The lower tier administrator has the ability to manage and control issues at the chat room level. The higher tier administrator has the ability to manage and control users and issues at the network level. User 1, whose nickname is indicative of a sexual interest in children, was a member of both moderator tiers. User 1 also has a bot—a computer program that performs automatic, repetitive tasks—set up that automatically posts a third-party link every minute to the Chat Room 1 chat room. The majority of these links lead to a site displaying an image or video involving depictions of minors engaged in sexually explicit conduct.

⁷ The real user name of User 3 is known to law enforcement but is being disguised in order to protect the ongoing investigation.

Transition from Network 1 to Network 2

12. Protocol A's network moderators are charged with the task of enforcing a particular network's rules and, in many cases, improving the network in various ways. In or about July 2018, several Network 1 administrators began closing Network 1 chat rooms focused on depictions of children engaged in sexually explicit conduct, including Chat Room 1, Chat Room 2⁸, and "Chat Room 8"⁹. On July 26, 2018, a post was made to the website "textuploader.com" informing users of a new, private Protocol A server, known as Network 2¹⁰, and how to access it. "Textuploader.com" is a website application that allows users to post/host text so that it can be easily shared with multiple users. The post discussed how Network 2 is a private Protocol A network offering a secure encrypted connection between a server and a web browser, the ability to mask a user's IP address information, and the ability to register a unique username. The post then provided detailed instructions for users regarding how to set up and access Network 2 on a user's Protocol A client.

13. SA Conrad observed that, around the time the Network 1 administrators began eliminating chat rooms dedicated to trafficking in child depictions of children engaged in sexually explicit conduct, the users who most frequently posted links to depictions of children engaged in sexually explicit conduct, like User 1, User 2, and User 3, migrated from Network 1 over to the newly-created Network 2. Many of the chat rooms that had been banned on Network

⁸ The real name of Chat Room 2 is sexually explicit and references the sexual exploitation of children. The real name is known to law enforcement but is being disguised in order to protect the ongoing investigation.

⁹ The real name of Chat Room 8 is known to law enforcement but is being disguised in order to protect the ongoing investigation.

¹⁰ The real name of Network 2 is known to law enforcement but is being disguised in order to protect the ongoing investigation.

1—such as Chat Room 1, Chat Room 2, and Chat Room 3¹¹—were recreated on Network 2 shortly after it was created. Many of the administrative users then created user names for Network 2 that were identical to those they’d used on Network 1.

14. On September 28, 2018, SA Conrad logged onto Network 2 and noticed the welcome message for Network 2. The welcome message listed the “Staff Members” associated with Network 2. User 1 was listed as a Network Administrator, User 2 was listed as a Network Administrator, User 3 was listed as the “CoOwner” of Network 2, User 4¹² was listed as a Network Administrator and User 5¹³ was listed as the “Host” of Network 2, meaning that these users would have had full network administrative privileges over that Network.

15. On September 18, 2018, at approximately 09:01 hours ET, in the Eastern District of Pennsylvania, SA Conrad logged into Network 2 and the Chat Room 1 chat room. While logged on, SA Conrad captured User 2 posting the following link at approximately 13:49 hours ET: “<https://www.120.zippyshare.com/v/JxXx7QdZ/file.html>”. SA Conrad accessed the link and verified that the video was child exploitation material. The twenty-nine second video portrays a naked pre-pubescent female and a naked adult female on the floor of a shower. The adult female begins to lick the pre-pubescent female’s nipples. The adult female then licks the pre-pubescent female’s vagina and begins to rub the girl’s vagina with her hand. SA Conrad downloaded the file to preserve it for evidentiary purposes.

¹¹ The real name of Chat Room 3 is sexually explicit and references the sexual exploitation of children. The real name is known to law enforcement but is being disguised in order to protect the ongoing investigation.

¹² The real user name of User 4 is known to law enforcement but is being disguised in order to protect the ongoing investigation.

¹³ The real user name of User 5 is known to law enforcement but is being disguised in order to protect the ongoing investigation.

16. On September 18, 2018, User 5 was also seen logging into Chat Room 1 on several occasions. While User 5 was logged into Chat Room 1, several users, including User 1, posted several links to child pornography. Some examples of the links posted during User 5 being logged in include: a picture of a naked pre-pubescent girl exposing the girl's vagina, a close-up picture of a pre-pubescent girl's vagina, a picture of a pre-pubescent girl wearing just a white t-shirt and exposing her vagina, and a picture of a naked pre-pubescent girl being vaginally penetrated by an adult male.

17. On January 29, 2019, at approximately 09:20 hours ET, in the Eastern District of Pennsylvania, SA Conrad logged into Network 2 and the Chat Room 1 chat room. While logged on, SA Conrad captured User 1's bot posting the following link at approximately 13:11 hours ET: "<http://funkyimg.com/i/2GvoD.jpg>". SA Conrad accessed the link and verified that the video was child exploitation material. The picture portrays a naked pre-pubescent sitting on a blue blanket spreading her legs and exposing her naked vagina. The logo "LS Models" is displayed in the upper right corner of the picture.¹⁴ SA Conrad downloaded the file to preserve it for evidentiary purposes.

18. On February 1, 2019, at approximately 09:47 hours ET, User 1 posted the following link: "<http://funkyimg.com/i/2Le9U.jpg>". SA Conrad accessed the link and verified that the video was child exploitation material. The picture portrays a pre-pubescent female that is naked from the waist down. An adult male is inserting his erect penis into her vagina. SA Conrad downloaded the image for evidentiary purposes.

¹⁴ In your affiant's training and experience, "LS Models" is a well-known child pornography series.

Transition from Network 2 to Network 3

19. On February 19, 2019, at approximately 10:48 hours ET, in the Eastern District of Pennsylvania, SA Conrad logged into the Network 2 server in an undercover capacity. SA Conrad noticed that there were significantly fewer users logged in to Chat Room 1 than he had observed during prior undercover sessions. At approximately 10:55 hours ET, a post was made to Chat Room 1 by [User 1]-afk,¹⁵ which stated the following, “We would like to inform everyone that [Network 2] will be closing soon for technical reasons. We invite everyone to join us at our new server” and then listed precise technical instructions for joining the new server, named “Network 3”. SA Conrad accessed Network 316 using the given instructions and thereafter observed a welcome screen for Network 3 that emphasized its lack of oversight. The welcome screen also listed users with identical user names as User 1, User 3, and User 4 listed as Network Administrators, which means these users would have administrative rights for Network 3. User 2 was also listed as members of Network 3.

20. On February 21, 2019, in the Eastern District of Pennsylvania, SA Conrad logged onto Network 3 in an undercover capacity and accessed Chat Room 1. At approximately 12:08:43 hours ET on February 21, 2019, User 2 posted the following link to the Chat Room 1 on Network 3: “<https://www114.zippyshare.com/v/Jhyj5crp/file.html>”. SA Conrad accessed the link on February 21, 2019, at approximately 14:49 hours ET. The video was confirmed to contain child exploitation material. The video is titled, “5yo kait dad exctasy”. It is thirty-eight

¹⁵ In your affiant’s training and experience, in Internet parlance, “afk” stands for “away from keyboard”. User 1 often writes posts that are automatically posted to the chat room, even though he might not physically be in front of the computer at that time.

¹⁶ The real name of Network 3 is known to law enforcement but is being disguised in order to protect the ongoing investigation.

seconds long and it portrays a pre-pubescent female forced to perform oral sex on an adult male. The girl makes an uncomfortable expression and the video transitions to slow motion to display the girl spitting out male ejaculate. SA Conrad downloaded the video for evidentiary purposes.

21. On March 4, 2019, in the Eastern District of Pennsylvania, SA Conrad logged onto Network 3 in an undercover capacity and accessed Chat Room 1 (a chat room with the same name as the one that had previously been hosted on Networks 1 and 2 that had again been recreated on Network 3). At approximately 19:51 hours ET on March 4, 2019, User 1 posted the following link to the Chat Room 1 chatroom on Network 3: “<http://funkyimg.com/i/2tS79.jpg>.”. SA Conrad accessed the link and verified that the picture was child exploitation material. The picture portrays a pre-pubescent girl naked from the waist down. The girl is spreading her legs exposing her naked vagina and has a pink dildo inserted into her anus. SA Conrad downloaded the image for evidentiary purposes.

22. On March 24, 2019, in the Eastern District of Pennsylvania, SA Conrad was logged onto Network 3 in an undercover capacity and accessed Chat Room 1. At approximately 16:25:42 hours ET on March 24, 2019, User 3 posted the following link to Chat Room 1 on Network 3: “<https://i.pinimg.com/736x/85/ee/2a/85ee2a63827d98427ede8c62bb6c5f80- - young-girls-kids-girls.jpg>”. SA Conrad accessed the link on August 20, 2019, at approximately 13:52 hours ET. The picture depicted two pre-pubescent girls in two-piece bathing suits wading in a river. SA Conrad downloaded the picture for evidentiary purposes. Following User 3’s post, another user commented, “Lovely pair of blondes [User 3].”

23. On May 7, 2019, at 11:31:02 hours ET, in the Eastern District of Pennsylvania, SA Conrad, acting in an undercover capacity as UC1, sent a message to Chat Room 1 on Network 3 asking whether anyone knew where User 2 had gone. At 11:36:52 hours ET, SA

Conrad received a private message from another Network 3 user telling him that User 2 was no longer logging in as User 2. After questioning this user, SA Conrad learned that User 2 was using a new username, namely “User 2 Alias”¹⁷.

24. SA Conrad reviewed previous log files from Network 3 communications and looked for the user name User 2 Alias. The log files revealed that the User 2 Alias began to appear around the time SA Conrad noticed that User 2 was no longer logging on. The log files reveal that on March 5, 2019, at 09:31:40 hours ET, User 2 Alias joined the Network 3 group Chat Room 1. On that same day, at 17:21:29 hours ET, User 2 Alias responded to another user by posting the following link, “http://img2208.imagevenue.com/aAfkjfp01fo1i-17901/loc514/572478405_152265265688_123_514lo.jpg”. SA Conrad accessed this link. It displayed a picture of a naked pre-pubescent girl on her knees with her buttocks in the air and ejaculate on her buttocks.

25. On May 8, 2019, at approximately 0451 hours ET, SA Conrad, while logged into Network 3 as UC1, was contacted by a Protocol A user that went by the nickname User 6¹⁸. User 6 was logged into Network 3 Chat Room 1, Chat Room 2, and Chat Room 4, each of which was dedicated to trafficking in child exploitation material.

26. On May 11, 2019, User 2 posted the following comment on Chat Room 1, “The previews have been removed from the settings in the back end of the web client. It was causing performance issues. It will be turned off for the foreseeable future until we can figure out a way that the previews are not directly routed through the back end.”

¹⁷ The real user name of User 2 Alias is known to law enforcement but is being disguised in order to protect the ongoing investigation.

¹⁸ The real user name of User 6 is known to law enforcement but is being disguised in order to protect the ongoing investigation.

27. On May 20, 2019, User 6 contacted SA Conrad (as UC1) again asking him if he had connection issues with Protocol A. During the course of the conversation, User 6 sent SA Conrad a message, "You ever seen this girl??" and then sent SA Conrad the following link to a video, "<https://www37.zippyshare.com/v/gn9KbFdN/file.html>". SA Conrad accessed the link on May 20, 2019, at approximately 1320 hours ET. The video was confirmed to contain child exploitation material. The video is twelve minutes and forty seconds long. The video begins with a pre-pubescent female wearing a t-shirt with a hoodie and jean shorts. The girl then inserts a blue hose like device into her mouth and she acts as if she is sucking on the hose. The girl then takes off her shorts and moves the camera to focus on her exposed vagina as she masturbates with her fingers. The girl switches from masturbating with her hand and the blue hose. The video ends with the girl putting her jean shorts back on. SA Conrad downloaded the video for evidentiary purposes.

28. User 6 told SA Conrad (as UC1) that he sent the video to UC1 because he "[w]as trying to get you to respond to me. And to show you that I am not a cop." At approximately 1346 hours ET, User 6 sent UC1 another video link, "<https://www.37zippyshare.com/v/diLyv0Bf/file.html>". SA Conrad accessed the link on May 20, 2019, at approximately 1353 hours ET. The video was confirmed to contain child exploitation material. The video is one minute and twenty seconds long. The video begins with a naked pre-pubescent girl sitting on the floor with her legs spread exposing her vagina. The girl masturbates with her fingers. The girl then moves closer to the camera which focuses on her vagina as she masturbates. SA Conrad downloaded the video for evidentiary purposes.

29. On May 28, 2019, at approximately 21:49 hours ET, User 1 posted the following link to the Chat Room 1 chatroom on Network 3:

“<https://www47.zippyshare.com/v/UX2rPlxJ/file.html>”. SA Conrad accessed the link and verified that the video was child exploitation material. The video is titled, “Selena-Rims-12.2018.1V7A2742.mp4” and is three minutes and four seconds in length. The video shows a pre-pubescent girl sucking on a lollipop. A naked adult male is lying on his back lifting his legs exposing his testicles and anus. The girl rubs her lollipop on his anus and then proceeds to lick his anus. The girl goes back and forth between licking her lollipop and licking his anus. The video concludes with the girl walking away and the viewer sees that she is just wearing underwear and socks. SA Conrad downloaded the video for evidentiary purposes.

30. On May 31, 2019, the User 1 bot posted a link to an image of a topless pre-pubescent female in her underwear. User 6 commented, “[User 1] that last one was amazing.” Later that same day, User 1 posted a link to a video with the name “Olga” after the link. The link accessed a video file that is thirty-eight minutes long, involving a pre-pubescent girl and an adult male. The adult male digitally penetrates the girl and has her perform oral sex on him. He also moves the girl in position to focus the video on her vagina and anus. After this link was posted, User 6 commented, “Great Vids [User 1].” Later User 1 then posted another link to a five-minute video involving two naked pre-pubescent girls. One of the girls is masturbating, while the other girl is sleeping. The older of the two girls then touches the vagina of the sleeping girl. The older of the two girls then performs oral sex on an adult male and then the sleeping girl. User 6 commented, “Damn amazing vid there [User 1] they just keep getting better.” SA Conrad accessed via link, viewed, and downloaded each video described in this paragraph for evidentiary purposes.

31. On June 21, 2019, at approximately 0805 hours ET, User 4 was logged into Chat Room 1 on Network 3. While User 4 was logged in, User 1’s bot posted a link which lead to a

an image involving a naked pre-pubescent female being vaginally penetrated by an adult male's penis. Another user posted a link to an image which lead to a picture of a naked pre-pubescent female on her hands and knees. The picture focuses on the vagina and anus of the girl. These links would have been available to any users logged onto Chat Room 1 on Network 3 at the time. SA Conrad downloaded these images for evidentiary purposes.

32. Through my investigation, this affiant has learned the following regarding the real identities of User 1 and User 6:

Identification of User 1

33. SA Conrad learned that the Network 1 Abuse Team collects information about each Protocol A subscriber on the network that registers a user name. It collects the user name, signup date and time, email address at the time of registration, registration IP address, last seen date and time, and most recent IP address. A Department of Homeland Security (DHS) summons was issued to the Network 1 Abuse Team for the subscriber information pertaining to User 1 and the User 1 bot. One of the members of the Network 1 Abuse Team responded with the following subscriber information:

User Name: XXXXX
Signup Date & Time: April 19, 2015 22:54:04 ET
Email Address: justme201312@gmail.com
Last Seen: 9/25/2018 @ approximately 09:08:40 ET
Last IP Address: 94.242.228.50
User Name: XXXXX
Signup Date: April 11, 2017 at 12:12:27 ET
Email Address: quietguy@ichigo.me
Last IP Address: 5.79.73.219

34. SA Conrad's investigation uncovered that the "justme201312@gmail.com" email address had at one point been associated with River City Media, a corporation that engaged in internet-based marketing. A DHS summons was issued to River City Media for information

pertaining to “justme201312@gmail.com”, the same email address associated with the Protocol A subscriber information obtained about User 1 from the Network 1 Abuse Team. River City Media provided the following information:

SignupDate: 2014-09-18 18:17:00
SignupIP: 50.252.40.217
First Name: Charles
Last Name: McCreary

35. SA Conrad sent a DHS summons to Textuploader.com for information about the IP address that uploaded the document instructing users how to logon to Network 2. . Textuploader.com provided SA Conrad with the IP address 2607:fb90:5f6b:64b3:2ab1:366a:6890:7832. According to the American Registry for Internet Numbers, as of March 1, 2019, that IP address was registered to T-Mobile. SA Conrad sent a DHS summons to T-Mobile for subscriber information for that IP address. T-Mobile responded with the following information:

Name: K C.K. HOT SHOT
Subscriber Address: 21734 Mossy Field Lane Spring, TX 77388

36. Charles McCREARY Jr is a lifetime registrant on the Texas Public Sex Offender Registry, and that registry currently lists McCREARY’s home address as 21734 Mossy Field Lane in Spring, Texas, 77388.

37. According to the Harris County, Texas Property Appraisal District, the residence at 21734 Mossy Field Lane in Spring, Texas is owned by one “Charles K. McCreary Jr.”

38. Surveillance of this residence has shown that McCREARY JR appears to be the sole resident of this property.

39. SA Conrad conducted a whois lookup for Network 3, the results of which provide registrar and registrant information pertaining to the “Network 3” domain name. According to

the whois lookup, the “Domain Registrar” for Network 3 is “NameSilo.com”. SA Conrad subsequently sent a Department of Homeland Security summons to NameSilo.com for account information pertaining to Network 3. NameSilo.com responded with the following information:

Created: 2018-10-23
Expires: 2019-10-23
Name: Henry Jones
Address: 23455 best st. Johnstown, PA 15901¹⁹
Email Address: quietguy@ichigo.me²⁰
Phone: 713-888-4858

The NameSilo.com response also stated that the subscriber purchased the domain for Network 3 using Bitcoin. The NameSilo.com response also stated that, on October 24, 2018, one day after the creation of Network 3, that network domain was being hosted on Network 2. In other words, the Network 3 domain was bought and created, however the domain was still being hosted on Network 2’s webserver. Network 3 did not move to its new webserver until February 10, 2019.

Identification of User 6

40. In the course of this investigation, SA Conrad learned that User 6 was utilizing the username NWNJDom on the application Kik. On May 21, 2019, SA Conrad sent a Department of Homeland Security Summons to Kik for subscriber information pertaining to the user NWNJDom. On May 24, 2019, Kik responded with the following information:

First Name: Scot
Last Name: F
Email: YourMasterDom@yahoo.com (Unconfirmed)
Registration Date: March 2, 2014 0839 hours UTC
Device Brand: Samsung
Device Model: SM-N950U

¹⁹ Subsequent investigation demonstrated that the address provided by NameSilo.com for the Registrant, Technical, Administrative, and Billing subscriber is fictitious.

²⁰ The email address provided by NameSilo.com is the same email address associated with the User 1 bot’s registration information on Protocol A.

41. In addition to the subscriber information, Kik also provided IP address logs. The initial IP address utilized to initiate communication with SA Conrad on 5/21/2019 at 1636 hours ET was 174.225.2.206. A query of the American Registry for Internet Numbers (“ARIN”) online database revealed that IP address 174.225.2.206 was registered to Cellco Partnership DBA Verizon Wireless, which comes back to Verizon Wireless. There were also several Wifi connections coming back to IP address 71.53.133.181, which according to ARIN was assigned to CenturyLink Communications, LLC.

42. On May 30, 2019, SA Conrad sent a Department of Homeland Security Summons to CenturyLink Communications, LLC. for subscriber information pertaining to IP address 71.53.133.181. CenturyLink responded on June 3, 2019, with the following subscriber information:

Name: Scot Fucito
Billing Address: 30 Sussex Street Newton, NJ 07860
Service Address: 30 Sussex Street Unit A Newton, NJ 07860
Service Establish Date: 02-03-2009

43. On May 30, 2019, SA Conrad sent a Department of Homeland Security Summons to Verizon Wireless for subscriber information pertaining to IP address 174.225.2.206. Verizon Wireless responded on June 12, 2019, with the following subscriber information:

Account Number: 986107112-1
Phone Number: 862-258-XXXX
First Name: Mariacecilia
Last Name: Fucito
Address: 30 Sussex Street Newton, NJ 07860

44. SA Conrad conducted a check for Scot FUCITO through CLEAR, a law enforcement database that compiles public records, which revealed the following:

Name: Scot A. Fucito
DOB: 4/22/1971
SSN: 148-76-XXXX

Address: 30 Sussex Street 7 Newton NJ, 07860

45. On June 3, 2019 SA Conrad ran FUCITO's name and DOB through the National Crime Information Center ("NCIC") database and found the following relevant information:

Offense Date 9/25/2007
Offenses: Criminal Attempt Sexual Assault-Vict 13-15 Y/O; Criminal Attempt
Endanger Welfare of Child
Disposition Date: 3/11/2009
Disposition: Guilty
Sentencing: 60 days in jail followed by 5 years probation

46. On June 3, 2019, SA Conrad accessed the Department of State system for passport information related to FUCITO. SA Conrad obtained a copy of FUCITO's 2012 United States passport application. The following information was obtained from FUCITO's passport application:


Name: Scot Alan Fucito
Address: 30 Sussex Street Newton, NJ 07860
Phone Number: 862-258-XXXX²¹
Occupation: Mobile Caterer

47. On July 1, 2019, User 6 asked SA Conrad to Skype chat. SA Conrad asked User 6 how to contact him via Skype, and User 6 stated to contact him on Skype at therisingphoenix360@gmail.com. SA Conrad utilized an undercover tablet to contact User 6. When SA Conrad connected with User 6, SA Conrad confirmed that User 6's likeness matched the photo from Scot FUCITO's driver's license.

²¹ The phone number listed on FUCITO's passport application is the same number tied to FUCITO's Verizon Wireless account.

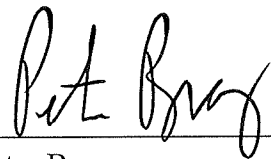
CONCLUSION

48. Based on the foregoing, there is probable cause to believe that MCCREARY, JR. and FUCITO have committed violations of 18 U.S.C. § 2252A(a)(2) and (b)(1) (Conspiracy to Receive and Distribute Child Pornography).



Joshua Conrad
Special Agent
Homeland Security Investigations

Subscribed and sworn before me this 27 day of August 2019, and I find probable cause.



Peter Bray
United States Magistrate Judge